A MAGYAR TUDOMÁNY ÜNNEPE

Magyar Tudományos Akadémia

MEGHÍVÓ

A Debreceni Egyetem Informatikai Kara szeretettel meghívja önt a

Magyar Tudomány Ünnepe

alkalmából rendezett

Andrej Dujella: Applications of Diophantine approximations algorithms in cryptanalysis of RSA

című tudományos előadására.

2017. november 24. 13:00
I130 Tanácsterem
4028 Debrecen, Kassai út 26.

Abstract:
To speed up the RSA decryption one may try to use small secret decryption exponent d. The choice of a small d is especially interesting when there is a large difference in computing power between two communicating devices. However, in 1990, Wiener showed that if d < n^(1/4), where n = pq is the modulus of the cryptosystem, then there exist a polynomial time attack on the RSA. He showed that d is the denominator of some convergent p_m/q_m of the continued fraction expansion of e/n, and therefore d can be computed efficiently from the public key (n,e).
In this talk, we will discuss similar attacks on RSA and its variants which use results and algorithms from Diophantine approximations, such as Worley's extension of the classical Legendre's theorem on continued fractions and LLL-algorithm for computing short vectors in lattices.

EMBERKÖZPONTÚ TUDOMÁNY
A MAGYAR TUDOMÁNY ÜNNEPÉNEK 2017-ES MOTTÓJA